The Simplest Security: A Guide To Better Password Practices

Refresher – Password Usage

Let's be honest, passwords are annoying. These days, we need a password or PIN everywhere. We have so many that we can't keep track of them all. We forget to update them; and when we do, it's difficult to come up with effective ones that we can still remember, so we procrastinate changing them for months, even years. We all know this is bad, but the alternative – the painful, irritating password creation and memorization process – is sometimes more than we can tolerate. There is hope! Passwords don't have to be complex cryptograms. A few simple methods can help make living with passwords a little easier.

While we may find them annoying, and even take them for granted, it is important to remember why passwords are important: passwords are often the first (and possibly only) defense against intrusion (Macgregor). They protect personal information – information we don't want anyone and everyone to know. In our personal lives, this means financial information, health data, and private documents. In a professional context, this may encompass anything considered crucial to the success of the organization: trade secrets, financial data, intellectual property, customer lists, etc.

Passwords are simpler and cheaper than other, more secure forms of authentication like special key cards, fingerprint ID machines, and retinal scanners. They provide a simple, direct means of protecting a system or account. For the sake of this article, we'll define a 'password' as a word, a phrase, or combination of miscellaneous characters that authenticates the identity of the user. Passwords are generally used in combination with some form of identification, such as a username, account number, or e-mail address. While a username establishes the identity of the user for the computer or system, the password, which is known only to the authorized user, authenticates that the user is who he or she claims to be. This means that their function is to "prove to the system that you are who you say you are" (Russell).

Password Cracking

While passwords are a vital component of system security, they can be cracked or broken relatively easily. Password cracking is the process of figuring out or breaking passwords in order to gain unauthorized entrance to a system or account. It is much easier than most users would think. (The difference between cracking and hacking is that codes are cracked, machines are hacked.) Passwords can be cracked in a variety of different ways. The most simple is the use of a word list or dictionary program to break the password by brute force. These programs compare lists of words or character combination against password until they find a match. If cracking codes seems like science fiction, search "password cracker" on Packet storm or Passwordportal.net. There are also numerous password cracking tools available that any average person can use. (For more information on password cracking tools, please see the SecurityFocus article Password Crackers - Ensuring the Security of Your Password.)

Another easy way for potential intruders to nab passwords is through social engineering: physically nabbing the password off a Post-It from under someone's keyboard or through imitating an IT engineer and asking over the phone. Many users create passwords that can be guessed by learning a minimal amount of information about the person whose password is being sought. (For more information on social engineering please see the SecurityFocus series Social Engineering Fundamentals) A more technical way of learning passwords is through sniffers, which look at the raw data transmitted across the net and decipher its contents. "A sniffer can read every keystroke sent out from your machine, including passwords" (University of Michigan). It's possible that someone out there has at least one of your passwords right now.

How To Choose Good Passwords

Now that we have established the importance of passwords and some of the ways in which they may be vulnerable to cracking, we can discuss ways of creating good, strong passwords. In creating strong, effective passwords it is often helpful to keep in mind some of the methods by which they may be cracked, so let's begin with what NOT to do when choosing passwords.

No Dictionary Words, Proper Nouns, or Foreign Words

As has already been mentioned, password cracking tools are very effective at processing large quantities of letter and number combinations until a match for the password is found, as such users should avoid using conventional words as passwords. By the same token, they should also avoid regular words with numbers tacked onto the end and conventional words that are simply written backwards, such as 'nimda'. While these may prove to be difficult for people to figure out, they are no match for the brute force attacks of password cracking tools.

No Personal Information

One of the frustrating things about passwords is that they need to be easy for users to remember. Naturally, this leads many users to incorporate personal information into their passwords. However, as is discussed in the Social Engineering Fundamentals, it is alarmingly easy for hackers to obtain personal information about prospective targets. As such, it is strongly recommended that users not include such information in their passwords. This means that the password should not include anything remotely related to the user's name, nickname, or the name of a family member or pet. Also, the password should not contain any easily recognizable numbers like phone numbers or addresses or other information that someone could guess by picking up your mail.

Length, Width and Depth

A strong, effective password requires a necessary degree of complexity. Three factors can help users to develop this complexity: length, width & depth. Length means that the longer a password, the more difficult it is to crack. Simply put, longer is better. Probability dictates that the longer a password the more difficult it will be to crack. It is generally recommended that passwords be between six and nine characters. Greater length is acceptable, as long as the

operating system allows for it and the user can remember the password. However, shorter passwords should be avoided.

Width is a way of describing the different types of characters that are used. Don't just consider the alphabet. There are also numbers and special characters like '%', and in most operating systems, upper and lower case letters are also known as different characters. Windows, for example, is not always case sensitive. (This means it doesn't know the difference between 'A' and 'a'.) Some operating systems allow control characters, alt characters, and spaces to be used in passwords. As a general rule the following character sets should all be included in every password:

- uppercase letters such as A, B, C;
- lowercase letters such as a, b,c;
- numerals such as 1, 2, 3;
- special characters such as $, ?, &; and
- alt characters such as µ, £, Æ. (Cliff)

Depth refers to choosing a password with a challenging meaning – something not easily guessable. Stop thinking in terms of pass*words* and start thinking in terms of *phrases*. "A good password is easy to remember, but hard to guess." (Armstrong) The purpose of a mnemonic phrase is to allow the creation of a complex password that will not need to be written down. Examples of a mnemonic phrase may include a phrase spelled phonetically, such as 'ImuKat!' (instead of 'I'm a cat!') or the first letters of a memorable phrase such as 'qbfjold*' = "quick brown fox jumped over lazy dog."

What may be most effective is for users to choose a phrase that is has personal meaning (for easy recollection), to take the initials of each of the words in that phrase, and to convert some of those letters into other characters (substituting the number '3' for the letter 'e' is a common example). For more examples, see the University of Michigan's Password Security Guide.

Extra Protection

All of the good password cracking programs include foreign words, backwards words, etc. And the easiest way to steal a password is by asking for it, so it's simpler to never give it away.

In some cases, a good password is enough protection to keep out intruders. In others, it's just a start. Encryption and one-time passwords add extra protection to systems. Encryption means garbling the password to protect from sniffers or other onlookers, through a particular scheme that can be deciphered from the other end of the connection. One-time passwords (S/key is the most commonly used) are just that. They can be used only once. This requires carrying a list of passwords or having a special password calculator or SecureCard, but can be a very reliable method of password security.

There are also certain behaviors that users should practice in order to maximize the effectiveness of their passwords. Users should avoid using the same password on multiple accounts. Doing this creates a single point of failure, which means that if an intruder gains access to one account, he

or she will have access to all of the user's accounts. Users should never disclose their passwords to anybody unless they know them to be authorized (i.e., systems administrators). Even then, passwords should only be disclosed in person (not over the phone or by e-mail) to a known, trusted source.

Users should exercise extreme caution when writing down or storing passwords. Stories of hackers obtaining passwords through shoulder-surfing and dumpster diving are not urban myths, they are real. Users should resist the temptation to write down passwords on Post-It notes stuck to their monitors or hidden under their keyboards. Instead, they should choose passwords that they will be able to remember – not an easy task given the complexity required of strong, effective passwords.

There are always extraneous circumstances where we must write down passwords. This is not recommended, but if it must be done, it should be done with forethought, not haphazardly. The extreme example of too many passwords is contract system administrators, who have multiple clients and machines. For these people, the only advice is to write down the phrases or some sort of related thought to jog your memory and put it on a piece of paper carried on your person. Maybe photocopy that and leave that stored in a safe place at home. Never put it on a Post-It. Never store it online. An obscured hint might be okay, but never the actual password or even an encrypted version.

Changing & Storing Passwords and PINs

In order to ensure their ongoing effectiveness, passwords should be changed on a regular basis. Changing passwords securely is fairly simple. Windows passwords are changed through the Control Panel and in UNIX, the 'passwd' command generally does the trick. A good rule of thumb is to change passwords as close to the actual account as possible. For example, if it's an ISP account, don't telnet through three other machines to change that password. If it's an office computer, users should be on that computer and not on a co-worker's when changing it. Don't let anybody watch while typing the old and new passwords. If at all possible, the password should be changed over a secure connection like a secure shell (SSH).

How often one should change passwords really depends on the account. Online financial accounts should be changed every month or two. Corporate network passwords should be changed every 3-4 months. A recent 2600 article recommended considering the "sensitivity of the resources which you are trying to protect" and suggested "enforcing password changes somewhere between once per fiscal year and once per fiscal quarter" (Thomas). Just use good judgment and don't be lazy. Changing a password is relatively quick and painless compared to the irritating and expensive process of combating identity theft.

Tips for Organizations and Network Administrators

Managers and administrators can enhance the security of their networks by setting strong password policies. Password requirements should be built into organizational security policies. Network administrators should institute by regular changes/updates of passwords. They should also regularly remind users of how easy it is for hackers to get their passwords through social

engineering and online attacks. New users should be taught about good password practices. Providing intranet resources on network security and password security can also be helpful. Finally, the organization's password policy should be integrated into the security policy, and all readers should be made to read the policy and sign-off on it.

Systems administrators should implement safeguards to ensure that people on their systems are using adequately strong passwords. They should set password expiration dates on all programs being run on the organization's systems. Keep a password history to prevent reuse, and lock of accounts after 3-5 password attempts. Keep the number of people in the organization who have these passwords as small as possible. The organization should also use newer versions of OSs that have more secure password files and authentication protocols. Keep your individual account passwords updated as well. Finally, when installing new systems, make sure default passwords are changed immediately.

New Year's Resolution

Obviously, passwords are just one piece of the puzzle. Other pieces are general user education, good physical security, plugging network holes, and installing strong firewalls. These provide much more global protection in the controlled corporate environment than passwords alone, but in areas where the only method of control users have is a PIN or password, the best thing we can do is be aware of security risks and keep up with their password controls.